UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/678,609	10/03/2003	Fred Cohen	529-000220US	1096

22798 7590 01/29/2007

QUINE INTELLECTUAL PROPERTY LAW GROUP, P.C.
P O BOX 458
ALAMEDA, CA 94501

EXAMINER	
CAO, DIEM K	

ART UNIT	PAPER NUMBER
2194	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	01/29/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/678,609	COHEN ET AL.	
	Examiner	Art Unit	
	Diem K. Cao	2194	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 October 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,4-9 and 11-23* is/are rejected.

7)☒ Claim(s) *3 and 10* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

WILLIAM THOMSON
SUPERVISORY PATENT EXAMINER

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *11/8/2004*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-23 are presented for examination.

2. The cross references related to the application cited in the specification must be updated (i.e. update the relevant status, with PTO serial numbers or patent numbers where appropriate).

Specification

3. The disclosure is objected to because it contains an embedded hyperlink and/or other form of browser-executable code on pages 3-5. Applicant is required to delete the embedded hyperlink and/or other form of browser-executable code. See MPEP § 608.01.

Allowable Subject Matter

4. Claims 3 and 10 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 1-2, 5-9, 13 and 15-17 are rejected under 35 U.S.C. 102(e) as being anticipated by Chieu et al. (U.S. 6,587,888 B1).

As to claim 1, Chieu teaches a method of modifying operation of an information system comprising:

- modifying a program execution call to first execute a wrapper logic module in user space instead of a requested program (Using the dummy ... assembly code in the interceptor code; col. 7, lines 36-58 and Since the DCOM interceptor ... client 150; col. 8, lines 12-14);
- examining a program execution request in light of one or more conditions (A DCOM server ... called function 106; col. 3, lines 31-36);
- selecting an action using the program execution request and the conditions (Part of the interceptor ... access calculator 250; col. 4, lines 47-48 and col. 8, lines 27-30);
- performing the action (external program that makes and returns the access decision to the interceptor; col. 8, lines 29-30); and
- selection a response using one or more of the program execution requests, the conditions and results of the action (Access is denied or granted; col. 5, lines 36-48);
- providing the selected response (control is passed to the targeted DCOM function 106 or control is passed to the interceptor's own access denied function; col. 5, clines 36-48).

As to claim 2, Chieu teaches providing a wrapper logic module able to receive information about a program execution request and able to select and perform an action based on

one or more conditions (construction of interception code for each DCOM function to be intercepted; col. 3, lines 6-10).

As to claim 5, Chieu teaches retaining permissions associated with the original program request, communicating with other decision processes or programs (col. 5, lines 24-43).

As to claim 6, Chieu teaches if a decision is made to execute the originally requested program, the wrapper replaces itself in a process space with the original requested program (col. 5, lines 36-38), and if a decision is made not to execute the originally requested program, the wrapper causes an alternative action to be taken (col. 5, lines 41-43).

As to claim 7, Chieu teaches the action is running a requested program (col. 5, lines 36-38). Examiner notes that the claim recites "and/or", thus, meeting one of action from the group of actions would meet the claim limitation.

As to claim 8, Chieu teaches the response comprises one or more deceptive responses, that do not correspond to what actually done by a wrapper (Access is denied or granted; col. 5, lines 36-48).

As to claim 9, Chieu teaches the wrapper can provide any response it is programmed to provide, regardless of what it actually does (Access is denied or granted; col. 5, lines 36-48).

As to claim 13, Chieu teaches a computer program product for use in an information system comprising a computer useable medium having computer readable program code embodied therein, the computer product further comprising

- computer readable code enabling a loadable operating system module able to intercept all program execution requests (A DCOM server interceptor program 200 intercepts the function calls produced by client 150; col.3, lines 31-32);
- wherein the module, after intercepting a program execution request, initiates logic to evaluate the program execution request and determine whether to grant, refuse to grant, or falsifies granting the program execution request depending on one or more parameters (The interceptor ... called function 106; col. 3, lines 33-36 and col. 7, line 61 – col. 8, line 36); and
- wherein the module, after intercepting a program execution request, returns either an accurate or an inaccurate response to the request depending on one or more parameter (access is granted or access is denied; col. 8, lines 30-34).

As to claim 15, Chieu teaches the module can selectively return false responses in response to a program execution request (access is denied; col. 8, lines 30-32).

As to claim 16, Chieu teaches the module can probabilistically return false responses in response to a program execution request (access is denied; col. 8, lines 30-32).

As to claim 17, see rejection of claim 1 above.

7. Claims 18-23 are rejected under 35 U.S.C. 102(e) as being anticipated by Deianov et al. (U.S. 6,529,985 B1).

As to claim 18, Deianov teaches a method comprising:

- ensuring a per-process program execution flag is at a control state at process initiation (execution flag 131; col. 7, lines 35-37 and The initialization … select process 107; col. 7, lines 7-20);
- checking the per-process flag at a first program execution request (When the interception module … wrapper; col. 7, lines 20-23 and the interception module first … execting; col. 8, lines 29-31);
- if the per-process flag is at a control state:

a) executing a control logic module instead of the first program (execute system call wrapper 125; col. 8, lines 25-26);

b) resetting the per-process flag to an uncontrol state (set the execution flag … executing; col. 9, lines 14-16);

c) the control logic module evaluating the program execution request (col. 2, lines 3-19);

d) the control logic module optionally generating one or more responses (provide access to the file system, processes can be prevented from manipulating files; col. 2, lines 8-10);

e) the control logic module optionally taking one or more actions (provide access to the file system, processes can be prevented from manipulating files; col. 2, lines 8-10); and

f) the control logic module optionally issuing a different program execution request (the system call was made by the wrapper; col. 8, lines 33-34);

- if the per-process flag is at an uncontrol state (The interceptor … executing; col. 8, lines 29-34)

a) executing the program execution request (execute the actual system call; col. 44-45); and

b) resetting the per-process flag to a control state (When the system call wrapper … not currently executing; col. 9, lines 25-27).

As to claim 19, Dianov teaches the control logic module executes in a protected user space (System call wrapper in user address space; col. 10, lines 24-26).

As to claim 20, Dianov teaches the control logic module consults other components in performing the evaluating and/or the generating (col. 8, lines 15-23).

As to claim 21, Dianov teaches a method of enhancing security in an information appliance comprising (col. 2, lines 3-19):

- modifying an execution function of the information processing system to initially call a program execution evaluation module (The present invention ... executes instead; col. 6, lines 16-27),
- determining whether or not to provide deception (When a process makes a system call ... of the calling process; col. 8, lines 15-28); and
- from the program execution evaluation module providing one or more of a set of available deceptions to entities for deception (provide access to the file system, processes can be prevented from manipulating files; col. 2, lines 8-10).

As to claim 22, see rejection of claim 19 above.

As to claim 23, see rejection of claim 21 above.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 4, 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chieu et al. (U.S. 6,587,888 B1) in view of Deianov et al. (U.S. 6,529,985 B1).

As to claim 4, Chieu teaches

- determining if the requested program would have been executed in normal operation (a function … is invoked; col. 7, lines 61-62);
- executing a wrapper in place of the original program (The interceptor code … function 106; col. 8, lines 10-12); and
- providing the wrapper with relevant information regarding the original execution request (A pointer … at runtime; col. 7, line 63 – col. 8, line 3).

Chieu does not teach setting a per-process flag indicating that a process is in a state where a program execution request should first execute the wrapper logic module. However, Deianov teaches setting a per-process flag indicating that a process is in a state where a program execution request should first execute the wrapper logic module (selected processes … wrapper 125; col.10, lines 35-53).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to apply the teaching of Deianov to the system of Chieu because it provides a method to selectively interception of systems call by specific processes (col. 3, lines 30-31).

As to claim 14, Chieu does not teach the module further comprises per-process tracking logic allowing the module to ensure that program execution in a process can only be executed from a wrapper. Deianov teaches the module further comprises per-process tracking logic allowing the module to ensure that program execution in a process can only be executed from a wrapper (col. 8, lines 29-55).

10. Claims 11, 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chieu et al. (U.S. 6,587,888 B1) in view of Wood et al. (U.S. 2004/0210771 A1).

As to claim 11, Chieu does not teach a response can be combined with other responses. However, Wood teaches a response can be combined with other responses (page 6, paragraph 50). It would have been obvious to one of ordinary skill in the art at the time the invention was made to apply the teaching of Wood to the system of Chieu because it provides a method for improving the security of information transactions over networks (page 1, paragraph 3).

As to claim 12, Wood teaches a response can be randomly and/or selectively generated based on time, use, or other environmental or fixed factors (page 4, paragraphs 37-38).

Conclusion

11. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO 892.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Diem K. Cao whose telephone number is (571) 272-3760. The examiner can normally be reached on Monday - Friday, 7:30AM - 3:30PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Thomson can be reached on (571) 272-3718. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

DC
January 22, 2007

WILLIAM THOMSON
SUPERVISORY PATENT EXAMINER